AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for managing discovery and ancillary protocols which lead to denial of service attacks ~~prohibiting iSCSI discovery sessions~~, comprising:

maintaining iSCSI standard support for all discovery sessions on all network portals, including returning a list of all targets on the network entity and all of the portal groups associated with each target;

providing send target discovery sessions as default behavior;

prohibiting send target discovery sessions as a system administrator option;

configuring discovery via supporting protocols external to the iSCSI protocol;

receiving an iSCSI login request;

determining whether a payload of said iSCSI login request contains a "SessionType=Discovery" key/value pair; and

when discovery sessions are disabled and said iSCSI login request contains said "SessionType=Discovery" key/value pair, rejecting said iSCSI login request.

2. (Original) The method of claim 1, wherein said iSCSI login request is rejected with a iSCSI status-class of "Target Error" and status-detail of "Session Type not Supported."

3. (Original) The method of claim 1, further comprising:

declaring a session type on said iSCSI login request.

4. (Original) The method of claim 1, further comprising:

when a session type is not explicitly declared on said iSCSI login request, assuming a session type is not a discovery session and specifying a specific target.

5. (Currently Amended) An apparatus for managing discovery and ancillary protocols which lead to denial of service attacks ~~prohibiting iSCSI discovery sessions~~, comprising:

maintaining iSCSI standard support for all discovery sessions on all network portals, including returning a list of all targets on the network entity and all of the portal groups associated with each target;

providing send target discovery sessions as default behavior;

prohibiting send target discovery sessions as a system administrator option;

configuring discovery via supporting protocols external to the iSCSI protocol;

means for receiving an iSCSI login request;

means for determining whether a payload of said iSCSI login request contains a "SessionType=Discovery" key/value pair; and

when discovery sessions are disabled and said iSCSI login request contains said "SessionType=Discovery" key/value pair, means for rejecting said iSCSI login request.

6. (Original) The apparatus of claim 5, wherein said means for rejecting said iSCSI login request comprising means for rejecting said iSCSI login request with a iSCSI status-class of "Target Error" and status-detail of "Session Type not Supported."

7. (Original) The apparatus of claim 5, further comprising means for declaring a session type on said iSCSI login request.

8. (Original) The apparatus of claim 5, further comprising:

when a session type is not explicitly declared on said iSCSI login request, means for assuming a session type is not a discovery session and means for specifying a specific target.

9. (Currently Amended) A computer-readable medium having computer-executable instructions for performing a method for managing discovery and ancillary protocols ~~prohibiting iSCSI discovery sessions~~, said method comprising:

maintaining iSCSI standard support for all discovery sessions on all network portals, including returning a list of all targets on the network entity and all of the portal groups associated with each target;

providing send target discovery sessions as default behavior;

prohibiting send target discovery sessions as a system administrator option;

configuring discovery via supporting protocols external to the iSCSI protocol;

receiving an iSCSI login request;

determining whether a payload of said iSCSI login request contains a "SessionType=Discovery" key/value pair; and

when discovery sessions are disabled and said iSCSI login request contains said "SessionType=Discovery" key/value pair, rejecting said iSCSI login request.

10. (Original) The computer-readable medium of claim 9, wherein said iSCSI login request is rejected with a iSCSI status-class of "Target Error" and status-detail of "Session Type not Supported."

11. (Original) The computer-readable medium of claim 9, wherein said method further comprising:

declaring a session type on said iSCSI login request.

12. (Original) The computer-readable medium of claim 9, wherein said method further comprising:

when a session type is not explicitly declared on said iSCSI login request, assuming a session type is not a discovery session and specifying a specific target.

13. (Currently Amended) A method for providing iSCSI target stealth operation, comprising:

maintaining iSCSI standard support for all discovery sessions on all network portals, including returning a list of all targets on the network entity and all of the portal groups associated with each target;

providing send target discovery sessions as default behavior;

prohibiting send target discovery sessions as a system administrator option;

configuring discovery via supporting protocols external to the iSCSI protocol;

providing a setting to individually enable/disable at least one of discovery sessions, SLP, iSNS, ICMP, and SNMP; and

when said discovery session, said SLP, and said iSNS are all disabled, providing a warning that an initiator must be statically configured to locate a target on an iSCSI entity.

14. (Original) The method of claim 13, wherein said enable/disable is distributed throughout a management application.

15. (Original) The method of claim 13, wherein said warning is provided to an administrator.

16. (Original) The method of claim 13, further comprising:

when all discovery mechanisms are disabled, providing said warning to a user.

17. (Currently Amended) An apparatus for providing iSCSI target stealth operation, comprising:

maintaining iSCSI standard support for all discovery sessions on all network portals, including returning a list of all targets on the network entity and all of the portal groups associated with each target;

providing send target discovery sessions as default behavior;

prohibiting send target discovery sessions as a system administrator option;

configuring discovery via supporting protocols external to the iSCSI protocol;

means for providing a setting to individually enable/disable at least one of discovery sessions, SLP, iSNS, ICMP, and SNMP; and

when said discovery session, said SLP, and said iSNS are all disabled, means for providing a warning that an initiator must be statically configured to locate a target on an iSCSI entity.

18. (Original) The apparatus of claim 17, wherein said enable/disable is distributed throughout a management application.

19. (Original) The apparatus of claim 17, wherein said warning is provided to an administrator.

20. (Original) The apparatus of claim 17, further comprising:

when all discovery mechanisms are disabled, means for providing said warning to a user.

21. (Currently Amended) A computer-readable medium having computer-executable

instructions for performing a method for providing iSCSI target stealth operation, said method comprising:

maintaining iSCSI standard support for all discovery sessions on all network portals, including returning a list of all targets on the network entity and all of the portal groups associated with each target;

providing send target discovery sessions as default behavior;

prohibiting send target discovery sessions as a system administrator option;

configuring discovery via supporting protocols external to the iSCSI protocol;

providing a setting to individually enable/disable at least one of discovery sessions, SLP, iSNS, ICMP, and SNMP; and

when said discovery session, said SLP, and said iSNS are all disabled, providing a warning that an initiator must be statically configured to locate a target on an iSCSI entity.

22. (Original) The computer-readable medium of claim 21, wherein said enable/disable is distributed throughout a management application.

23. (Original) The computer-readable medium of claim 21, wherein said warning is provided to an administrator.

24. (Original) The computer-readable medium of claim 21, wherein said method further comprising:

when all discovery mechanisms are disabled, providing said warning to a user.